

AUSA Assigned: JHH

SEALED

FILED IN THE  
U.S. DISTRICT COURT  
EASTERN DISTRICT OF WASHINGTON

MAR - 8 2011

JAMES R. LARSEN  
SPOKANE, WASHINGTON DEPUTY

*In re: Criminal Complaint Kevin William Harpham  
(Stevens County)*

**AFFIDAVIT**

STATE OF WASHINGTON     )  
  :SS  
County of Spokane         )

John T. Slack, being first duly sworn on oath, deposes and states:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed for approximately 2 years. I attended the FBI Academy in Quantico, Virginia from February 2009 through July 2009. As a SA I am responsible for assisting in investigations of federal crimes, including crimes involving the use, placement, and possession of improvised explosive devices. I am currently assigned to the Seattle Division, Spokane Resident Agency/Inland Northwest Joint Terrorism Taskforce (INJTTF) of the FBI where I primarily investigate terrorism matters. I have assisted in the investigation of several domestic terrorism matters, including white supremacy and militia matters. I participate in weekly briefings on domestic terrorism investigations in this region and have had numerous discussions with the primary case agents for such matters.

Affidavit of John T. Slack

1 of 34

P10308DD.JHD.wpd

SEALED

For the approximately five years prior to becoming a Special Agent, during the period from October 2005 to February 2009, I was employed by the FBI as an Intelligence Analyst (IA), with the Counterterrorism Division. As an IA, I was assigned to the Counterterrorism Watch, a 24-hour Watch Center responsible for assisting FBI field agents in immediate incident response, to include domestic bombings, overseas attacks, and other threat matters investigated by the FBI. During the tenure of my FBI employment, I have worked on a variety of domestic and international terrorism matters.

2. As a FBI SA, I have received training and experience in the processing of crime scenes, drafting and executing search warrants, and investigating a variety of other violations of the federal criminal laws. Although investigating computer-based crimes is not my primary responsibility, I have personally participated in the execution of numerous search warrants involving the search and seizure of computers and related equipment.

3. As set forth in greater detail below, on January 17, 2011, an Improvised Explosive Device (IED) was discovered at the Northeast corner of Main and Washington Streets in Spokane, Washington, prior to, and along the planned route of, the Martin Luther King Jr. Day Unity March. The IED contained

Affidavit of John T. Slack

2 of 34

P10308DD.JHD.wpd

approximately 128 fishing weights, with a coating containing brodifacoum (an anticoagulant and an active ingredient within some rodenticides), inside a steel pipe which was welded onto a steel base plate (similar to a mortar tube). Law enforcement officers believe the IED was placed in order to expel the fishing weights as shrapnel into the march participants as they passed by, causing death or serious bodily injury, and into the public street and nearby businesses, causing property damage .

4. The purpose of this Affidavit is to set forth sufficient factual support for the issuance of a Criminal Complaint charging Kevin William Harpham with violations of Title 18 U.S.C. § 2332a (use of a weapon of mass destruction and attempts / conspiracy to do so) and Title 26 U.S.C. § 5861(d) (possession of an unregistered firearm defined as a destructive device) and a warrant for his arrest.

#### STATEMENT OF PROBABLE CAUSE

5. The facts and opinions set forth on this Affidavit have been derived from my above-described training and experience, as well as my personal participation in this investigation and from information provided to me by FBI agents / employees and from state and local law enforcement personnel.

Affidavit of John T. Slack

3 of 34

P10308DD.JHD.wpd

6. Because this Affidavit is being submitted solely for the purpose of establishing probable cause for the issuance of a search warrant / arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to support the issuance of the requested search warrant / arrest warrant.

7. The FBI's investigation of the instant matter has revealed that on January 17, 2011, at approximately 9:30 a.m., a suspicious backpack was discovered near the Northeast corner of the intersection of Main and Washington Streets in downtown Spokane, Washington. Individuals working in the area reported that the backpack, which had been placed near the intersection prior to and along the route of a planned Martin Luther King Jr. Day Unity March, contained suspicious wires. The Spokane County Sheriff's Office Explosives Disposal Unit responded and discovered that the backpack contained an Improvised Explosive Device (IED). The Disposal Unit disrupted the IED and turned over the IED components to FBI Special Agent Bomb Technician (SABT) Leland C. McEuen.

- a. SABT McEuen has been a certified FBI SABT since November 29, 2002. As a SABT, he has participated in bombing investigations in the United States and internationally. SABT McEuen has completed a 90-day deployment to Iraq where he conducted multiple post-blast investigations. Additionally, SABT McEuen is a post-blast

Affidavit of John T. Slack

4 of 34

P10308DD.JHD.wpd

investigations instructor and has taught numerous training classes, including classes relating to explosive and IED recognition, large vehicle bomb investigations, and large vehicle bomb countermeasures.

8. SABT McEuen observed the components of the IED from inside the backpack and concluded that all the parts for a functioning IED appeared to be present: a power source, a triggering device, an expelling/lifting charge, and shrapnel. Based on information from SABT McEuen and personnel from the FBI laboratory, your Affiant knows that the IED consisted of a steel pipe, containing a charge and shrapnel (ie: fishing weights), all enclosed within a wooden box and a powering/triggering system.

- a. The main charge assembly consisted of a steel pipe, approximately 3.5" in diameter, with a hole, approximately 0.25" in diameter, drilled near its base. The steel pipe was welded to a roughly-cut steel base plate, approximately 6.5" X 4.0" and approximately 0.4" thick. Both the steel pipe and steel base plate appeared to be heavily rusted. The steel pipe and base plate were secured to a wooden base, approximately 7" X 4.5" and approximately 1.5" thick, by four silver-colored, rounded Phillips-headed screws.
- b. Two insulated wires (one appearing black and red and the other appearing black and blue, both approximately 25 gauge) lead through the approximately 0.25" in diameter hole and connected to a model rocket igniter (MRI), inserted into the main charge.
- c. The FBI laboratory chemically identified the main charge as being a low explosive black powder. SABT McEuen determined there was

Affidavit of John T. Slack

5 of 34

P10308DD.JHD.wpd

approximately 100 grams of the black powder, contained in a plastic bag, inside the steel pipe.

- d. The plastic bag containing the black powder was itself contained in a white polyvinyl chloride (PVC) pipe 2" end cap wrapped with silver duct tape. The open end of the end cap was facing toward the base of the steel pipe. The 2" end cap and duct tape had a notch cut in them to allow wires to lead through the notches to the MRI inserted into the main charge.
- e. Within the steel pipe, taped on top of the PVC 2" end cap, was a 3" yellow knock-out plug. Atop the yellow knock-out plug was a clear plastic bag containing 128 quarter-ounce fishing weights. The weights were coated in a green substance, determined to contain brodifacoum (an anticoagulant and an active ingredient within some rodenticides).
- f. In addition, a circular cardboard cut-out, approximately 3.5" in diameter with U.S. Postal Service priority postage lettering, was also discovered inside the steel pipe.
- g. The IED had been placed within an open-ended wooden box, approximately 7" X 4.5" X 8". The sides of the box were made of wood approximately 0.5" thick and the wooden base is approximately 1.5" thick. Screws holding the box together were green-colored, flat Phillips-head screws. The wooden box itself was wrapped in numerous t-shirts, and taped in place inside the backpack.
- h. Components of the IED's triggering / powering system were also inside the backpack. The triggering system consisted of an Audiovox remote car starter/alarm receiver, which could receive a signal from a remote matching transmitter. The car starter/alarm receiver was powered by two 6-volt Rayovac lantern batteries, with a model number 945.

9. Based on SABL McEuen's training and experience the IED was designed to function by wireless trigger, to activate a relay switch allowing power to ignite the MRI, thereby igniting approximately 100 grams of black powder, which in turn would expel the lead weights at a high rate of speed, similar to the action of a mortar. Based on SABL McEuen's training and experience the position of the backpack containing the IED at the Northeast corner of the intersection of Main and Washington Streets would have caused death or serious bodily injury to the participants in the march and caused damage to the two business located across the street, on the Southeast and Southwest corners of the intersection, from where the IED was discovered, as well as to Main and Washington Streets. This would have caused these businesses to be closed for a period of time and adversely affected interstate commerce in addition to reducing business because of the public stigma associated to a bombing, had it occurred.

- a. Based on your Affiant's personal knowledge and on information from FBI TFO Richard Watson, Eye Care Center, a general optometry business located on the Southeast corner of Main and Washington Streets buys, sells, and uses items obtained from several distributors located outside the State of Washington. In addition the business was closed for 3-4 hours on January 17, 2011, and appointments were canceled, as a result of law enforcement's discovery of the backpack containing the IED.

Affidavit of John T. Slack

7 of 34

P10308DD.JHD.wpd

- b. Based on your Affiant's personal knowledge and on information from FBI TFO Watson, Hill's Restaurant, a restaurant and bar located on the Southwest corner of Main and Washington Streets buys, sells, and uses items obtained from nationwide distributors located outside the State of Washington. According to the owner of Hill's Restaurant, business noticeable declined the two days following January 17, 2011, which he attributes to the discovery of the backpack containing the IED.
- c. The intersection of Main and Washington Streets is a public thoroughfare used by commercial vehicles to transport goods in interstate commerce.

10. Analysis by the INJTTF and the FBI Laboratory identified the following components included in the backpack and device:

- a. Swiss Gear Backpack - Model SA9104;
- b. 3.5" diameter welded steel tube with a hole drilled near the base;
- c. Slip line lead oval fishing weights marked ¼ ounce;
- d. 2" Genova schedule 40 PVC threaded end cap, with the rim of the cap having been ground down;
- e. Audiovox Prestige remote car starter, model APS620N, including various wires and fuses;
- f. Automotive relay switch;
- g. 3" Cherne Industries Incorporated yellow knock out plug;
- h. Two (2) Rayovac brand 6v batteries, model 945, lot #IGOH1X 0614;

Affidavit of John T. Slack

8 of 34

P10308DD.JHD.wpd



- i. Nine (9) T-shirts of varying size and description;
- j. Circular cut out from a United State Postal Service Priority Mail package;
- k. Red indicator light with two electrical connectors;
- l. White plastic zip tie with locking mechanism missing;
- m. White tape, 1 inch wide;
- n. Silver duct tape;
- o. Masking tape;
- p. Black electrical tape;
- q. White duct tape;
- r. Black powder (approximately 100 grams);
- s. Box fabricated with wood and screws;
- t. Model rocket igniter, and
- u. Automotive-type wiring of various colors with gauges ranging from approximately 14-25 gauge, wire connectors, spade connectors, and miscellaneous crimps.

11. In addition to the components included in the backpack and device, the FBI Laboratory found trace evidence on and inside the Swiss Gear backpack, including:

Affidavit of John T. Slack

9 of 34

P10308DD.JHD.wpd

- a. Caucasian body hair;
  - b. Caucasian or Caucasian characteristic head hair (some of which exhibit characteristics of having been artificially treated and/or bleached);
  - c. Animal hairs consistent with dog and cat hairs;
  - d. Various types and colors of textile fibers; and
  - e. Male and female DNA on various component items, to include:
    - i. The handle and shoulder strap of the black backpack;
    - ii. T-shirts;
    - iii. Duct tape;
    - iv. Electrical tape;
    - v. White tape;
    - vi. Masking tape; and
    - vii. Hair
12. On January 18, 2011, the FBI publically offered a \$20,000 reward for information leading to the arrest of the perpetrator(s) of the manufacture and attempted detonation of the IED. The FBI received dozens of tips from the public and developed other investigative leads independently. In following those leads

Affidavit of John T. Slack

10 of 34

P10308DD.JHD.wpd

the FBI eliminated several possible suspects, but did not have sufficient information to eliminate others.

13. The current investigation has revealed that items discovered in the backpack could have been obtained in Stevens County, Washington, specifically the city of Colville, Washington. Such items include two unique t-shirts that had been used to wrap the IED in the backpack. Each t-shirt had printing on it commemorating an event hosted in Stevens County, Washington, namely: (1) the Spring 2009 Chewelah, Washington after-school production of Treasure Island and (2) the June 2010 American Cancer Society Relay for Life event held in Colville, Washington.

14. The current investigation confirmed purchases of items, similar, if not identical, to those utilized in the IED, at retail outlets in the Colville, Washington area. On February 12, 2011, FBI SA Craig Noyes located quarter-ounce fishing weights, sold in packs of 10, which appeared similar to those used in the IED for sale at the Wal-Mart store in Colville, Washington. Based on an FBI analysis of information provided by Wal-Mart relating to the sales of such weights at 72 Wal-Mart stores in the Pacific Northwest during October 30, 2010 - January 25, 2011, the Wal-Mart store in Colville, Washington had an unusually high amount of the weights sold during a one-week period in November, 2010.

Affidavit of John T. Slack

11 of 34

P10308DD.JHD.wpd

- a. On November 1, 2010, 40 weights (4 packs of fishing weights), Kraft brand Jet-Puffed Marshmallow Creme, vitamin D milk, a few food items, and a Farberware-brand food chopper were purchased with cash.
- b. On November 3, 2010, 60 weights (6 packs of fishing weights) were purchased with cash.
- c. On November 7, 2010, 30 weights (3 packs of fishing weights), Kraft brand Jet-Puffed Marshmallow Crème, and vitamin D milk were purchased using a bank card subsequently determined through FBI investigation of bank records to have been issued to Kevin William Harpham.

In total, the three above-described purchases totaled 130 weights, whereas 128 weights were located in the IED. Additionally, none of the three purchases include any other fishing-related items. In mid-February, 2011, FBI IA Pulcastro contacted the Washington State Fish and Wildlife Licensing Division and was advised that Kevin William Harpham last purchased a fishing license on July 11, 2007 in Burlington, WA.

15. On February 12, 2011, FBI SA Noyes identified multiple Rayovac brand 6v batteries, model 945, for sale at the Big R store in Colville, WA. SA Noyes observed that one of the batteries on the shelf was the same lot number, IGOH1X0614, as both Rayovac batteries utilized in the IED. Sales records provided by Big R identify a cash purchase of two Rayovac brand 6v batteries,

Affidavit of John T. Slack

12 of 34

P10308DD.JHD.wpd

model 945, on November 2, 2010. The sales records also indicate that a 35-foot roll of 18-gauge wire was purchased along with the batteries.

16. On February 18, 2011, FBI Task Force Officers (TFO) Darin DeRuwe and Darrell Bone determined that 3" Cherne knock-out plugs and 2" Genevo end caps are sold at the Colville Hardware Do It Center. Based on records from the Colville Hardware two cash sales were identified where both items were purchased together (with no other items listed on the sales receipt) on both November 7, 2010 and November 13, 2010. Mr. David Hubbard, the owner of Colville Hardware, advised that these transactions were unusual to him because the items would not normally be used together and are intended for completely different systems.

17. Between February 25, 2011 and March 4, 2011, FBI SA Michelle Taylor conducted online open-source searches related to Kevin Harpham and identified an individual using the online moniker "Joe Snuffy" for postings on the website [www.vnnforum.com](http://www.vnnforum.com), the Vanguard News Network Forum, which is a known white-supremacist website. Your Affiant believes "Joe Snuffy" is the same individual as Kevin Harpham based on the content of the posts on the forum.

Affidavit of John T. Slack

13 of 34

P10308DD.JHD.wpd

- a. On February 16, 2009, "Joe Snuffy" states, "I live near Colville, WA north of Spokane about an hour on 395"

This general description is consistent with the location of Harpham's premises located at 1088 Cannon Way, Colville, Washington.

- b. On May 21, 2006, "Joe Snuffy" states, "I want to build a cabin on 10 acres I bought in 97 after I sell this house and become a free man again. The cabin I have laid out is about 20 by 20 and I want a basement under it."

Stevens County property ownership and tax records indicate property owned by Kevin Harpham, parcel number 2220500, 1088 Cannon Way, Colville, Washington, 99114, was purchased on May 13, 1997 and consists of 9.83 acres.

- c. On March 30, 2008, a user identified as "Kevin\_Harpham" posted the following request to a moderator: "All I did was try to change my email and it screwed up everything. I could not PM anyone or even post so I reregistered and then realized that there was a verification for email change sent to my mailbox but it never told me before hand. I then tried to follow the verification link to reestablish Joe Snuffy but was still unable to do so. If a mod could clear this up for me or at least tell me what to do to fix it I would much appreciate it and get rid of this Kevin Harpham guy too, if you desire."

18. The following is a sample of "Joe Snuffy's" posts to the website

[www.vnnforum.com](http://www.vnnforum.com) :

- a. On June 17, 2006, Joe Snuffy posted to the thread "Hedi Klum had a mulatto moolie", "As long as she doesn't have any white kids (and lets hope she don't) she is already dead. The whites that live through

Affidavit of John T. Slack

14 of 34

P10308DD.JHD.wpd

this Jewish virus that is coming to a head will be much healthier than the herd of the past. As long as we are not exterminated (and we won't be) the Jews will have been one of the better things that ever happened to our race. We will evolve, we will live and we will be better for it.:Cheers:"

- b. July 5, 2006, Joe Snuffy posted to the thread "How Would ZOG React to Revolution at Home?" in response to the posting by Todd in FL of: "That's why lone wolfism is ideal in the new revolution...Lone wolves can do things that the govt is not ready for too." Joe Snuffy responded, "Todd, having just 2 people working together is far more effective than a single individual. A cell doesn't require a higher authority."
- c. On August 11, 2007, Joe Snuffy asked what is the legal limit of ammunition someone can possess at their home in WA.
- f. On August 13, 2007, Joe Snuffy stated he owns an AR-15, but also wanted to purchase an AK-47 type rifle. He also said, "Also does one see a use for a sub-machine gun like a .45 or 9mm in a WN (White Nationalist) war chest?"
- g. March 27, 2008, Joe Snuffy posted that he is storing bulk flour in 25 lbs buckets.
- h. On April 2, 2008, Joe Snuffy posted that he buys jeans at "Kostco," shoes at Big Five, wears t-shirts in the summer and t-shirts and a sweatshirt in the winter, which he buys from yard sales. He purchased a "camo" hat from Wal-Mart.
- i. On April 15, 2008, in response to the posting by Metal Warrior of "5) Pick up long-range scoped firearm, begin to remove individuals who head up depts., orgs and businesses which oppress, repress or destroy White people..." Joe Snuffy posted, "If any of you choose to do #5 please practice holding the camcorder still before you do the real

thing otherwise I will accuse you of being a Arab in the comments section."

- j. On May 23, 2008, Joe Snuffy posted, "Thanks Daniel but I am not interested in being a part of ANSWP (American National Socialist Workers Party). I am interested in meeting people close to me unless they are the kind of people that are waiting for Jesus to come back, then I can do without. Do you know anyone up here in northeastern Washington."
- k. On January 15, 2011, Joe Snuffy's last identified posting to this site occurred.

19. On February 14, 2011, IA Pulcastro conducted checks in law enforcement fee-for-service databases and discovered Kevin William Harpham was born on May 1, 1974, is assigned social security account number 531-02-8624, and has been issued Washington Driver's license number HARPHKW264KA that depicts Harpham's photograph, a copy of which photograph IA Pulcastro has obtained. IA Pulcastro also determined that Harpham was a member of the United States Army from 1996-1999.

20. On February 25, 2011, a court order was delivered on the Armed Forces Institute of Pathology (AFIP) to produce the Armed Forces Repository of Specimen Samples for the Identification of Remains (AFRSSIR) specimen sample of Kevin William Harpham. This specimen was provided to the FBI on February

Affidavit of John T. Slack

16 of 34

P10308DD.JHD.wpd



28, 2011. Analysis by the FBI Laboratory revealed the presence of nuclear DNA from three or more individuals on the handle and shoulder straps of the black backpack. The nuclear DNA obtained from the AFRSSIR specimen sample for Kevin Harpham was compared to these nuclear DNA samples and Harpham was identified as potentially the major contributor -- the FBI Laboratory advised the random match probabilities are 1 in 10 million from the Caucasian population, with a confidence interval between 1 in 1 million and 1 in 100 million. Analysis also either excluded Harpham as a major contributor to other trace nuclear DNA obtained from other components or no comparison information could be provided. The nuclear DNA analysis also identified female nuclear DNA on various t-shirts and duct tape found within the backpack. Additionally, the analysis revealed the presence of nuclear DNA (not matching Harpham) from three or more individuals on the T-shirts used to wrap the IED.

21. The FBI Laboratory also conducted mitochondrial DNA (mtDNA) analysis on five hairs found inside the backpack and compared these findings with mtDNA obtained from the AFRSSIR specimen sample for Kevin Harpham. The mtDNA sequences obtained from specimens from two hairs and Harpham are the same across the regions obtained in common for the three samples. Therefore, Harpham

Affidavit of John T. Slack

17 of 34

P10308DD.JHD.wpd

cannot be excluded as the source for the two hairs. The FBI Laboratory advised the mtDNA sequence obtained from the three specimens has been observed in 8.63% of the Caucasian population (upper bound frequency estimate ).<sup>1</sup> The analysis revealed Harpham can be excluded as being the source for two other hairs and is inconclusive in regards to the last hair.

22. On February 16, 2011, FBI SA Ryan Butler received subpoena results from Amazon.com. The results revealed Harpham has made multiple purchases via the Internet of video equipment. On November 15, 2010, he purchased a Panasonic Lumix model DMC-ZS7 digital camera. This camera has the capability to record High Definition video and is equipped with Power Optical Image Stabilizer. On November 15, 2010 and January 13, 2011, Harpham purchased two 8GB memory cards, compatible with the digital camera. For each purchase, Harpham used the email address [kevinharpham@hotmail.com](mailto:kevinharpham@hotmail.com) and the I.P. address 209.173.254.189. The I.P. is registered to Internet Xpress (Internet Express) and locates to Colville,

---

<sup>1</sup> The upper bound frequency estimate is based on a 95% confidence interval and gives an estimate of the highest percentage of individuals in each population group expected to have the same profile as the three samples.

Washington. Bank of America records show that Harpham paid monthly bills to Inter XP (Internet Express).

23. On February 15, 2011, IA Pulcastro contacted Avista Corporation and obtained utility service records for accounts listed and/or billed in the name of Kevin Harpham. According to these records, Harpham has two active accounts with electronic billing utilizing kevinharpham@hotmail.com. Both accounts list 1088 Cannon Way, Colville, Washington as the service location. On March 6, 2011, your Affiant checked the Stevens County Assessor's Office via the internet and saw that parcel number 2220500, having an address of 1088 Cannon Way, Colville, Washington, 99114, is owned by Kevin W. Harpham. The parcel is described as having a single family residence, with a mailing address of P.O. Box 126 Kettle Falls, Washington, 99141. The parcel is 9.83 acres with a single family residence built in 2007 and a lean-to, farm utility building.

24. The Assessor's office image of the premises shows two buildings and a dirt (parking) lot on the property. Associated with parcel 2220500 is parcel 4012278, which is described as an ATCO manufactured home, 14' X 64', built in 1974. Kevin W. Harpham is listed as the owner of parcel 4012278 with a mailing

Affidavit of John T. Slack

19 of 34

P10308DD.JHD.wpd

address of P.O. Box 126 Kettle Falls, Washington, 99141. Parcel 4012278 is listed as having 0.00 acres.

- a. On March 4, 2011, IA Pulcastro contacted Avista Corporation and obtained utility service records for accounts listed and/or billed in the name of Roy Hinson. According to these records, Roy Hinson has an active electric service account in his name at 1088 Cannon Way trlr, Colville, WA, 99114 with a listed mailing address of PO Box 264, Addy, Washington, 99101, telephone 509-684-6362. Service to this trailer house was established on December 17, 2009.
- b. The investigation has revealed that Roy Hinson is fully identified as Roy Albert Hinson, having a date of birth March 7, 1938, a social security number 251-56-6995, and Washington Driver's license HINSORA621DG.
- c. Based on information from FBI SA Joe Cleary who has driven past the premises located at 1088 Cannon Way, Colville, Washington, it described as an approximate ten acre parcel with a residence and attached lean to, with a manufactured trailer home approximate 14' x 64' located on the premises. The premises can be accessed by traveling north on US 395, turning west on 12-mile Road, north of Addy, Washington. After crossing railroad tracks and a bridge, turning right on Townsend-Sackman Road. After approximately 300 meters, turning left at the first road, and immediately turning right on Cannon Way. The premises is approximately 150 meters on the right. At the entrance to the driveway is a blue entrance sign with 1088 in white numbers. The premises is set approximately 25 meters from Cannon Way and is white in color.

25. On February 14, 2011, SA Ryan Butler conducted checks with the Washington State Vehicle Registration. Records show that Harpham is the

Affidavit of John T. Slack

20 of 34

P10308DD.JHD.wpd

registered owner for three vehicles:

- a. a 1989 Blue Toyota Camry, license plate 260UMG, VIN: 4T1SV24E0KU063649;
- b. a 1991 Silver Toyota Camry, license plate 466PYF (expired), VIN: JT2SV21J7M0039180; and
- c. a 1989 Maroon Toyota Camry, license plate 868RAQ (expired), VIN: JT2SV24E0K3354199.

On March 4, 2011, SA Ryan D. Butler received store security video from the Colville, Washington Wal-Mart for purchases made on December 21, 2010 and February 28, 2011, both of which purchases were made with a debit card for Kevin Harpham's account at Bank of America. SA Butler reviewed both videos and observed a white male, appearing to be Kevin Harpham, make both purchases. In both instances, the male departed the store and drove away in a light-colored, four door sedan, generally matching the description of a Toyota Camry.

26. On February 16, 2011, FBI SA Cleary obtained transactional records from Costco for items purchased utilizing Kevin Harpham's Costco membership card number. These records identified recent purchases of dog and cat food. On January 15, 2011, there was a purchase of 80 pounds of dog food and on February 15, 2011, there was a purchase of 100 pounds of cat food. On February 19, 2011,

Affidavit of John T. Slack

21 of 34

P10308DD.JHD.wpd

FBI TFO Mark Dean, while conducting surveillance, observed a male walking on the premises, near the residence at 1088 Cannon Way, with at least two dogs.

27. On March 7, 2011, Senior SA Darrell Bone, Bureau of Alcohol, Tobacco, and Firearms, completed checks in the National Firearms Registration and Transfer Records for Kevin William Harpham and determined there is no firearm, including a destructive device by definition, registered to him. Based on your Affiant's training and experience, and discussions with SABT McEuen, the IED described herein is a destructive device.

28. Based on my training and experience, and discussions with trained law enforcement members of the INJTTF, I know that individuals who place and detonate IEDs, or attempt to do so, commonly conduct pre-operation planning, which often include:

- a. Physically inspecting potential detonation locations;
- b. Videotaping potential detonation locations;
- c. Purchasing and viewing videos and films regarding public gatherings, marches, and parades;
- d. Identifying potential escape routes, and
- e. Conducting on-line research for every aspect of the operation, such as using websites like Google Maps to obtain street and aerial maps of

Affidavit of John T. Slack

22 of 34

P10308DD.JHD.wpd

the detonation site and escape routes, and visiting other internet sites to choose targets and learn bomb making techniques.

29. Based on your Affiant's training and experience, and discussions with other trained law enforcement members of the INJTTF, I know that it is common for individuals involved with hate groups and white supremacy-type groups to keep items relating to their beliefs, the white supremacy cause, and targets or potential targets, to include diaries, calendars, books, pamphlets, magazine, newspaper articles, pictures, movies, videos, and other literature in electronic and physical form; and that they keep these items for ready access and use in their homes, on their property, in their vehicles, and in storage areas.

30. Based on my training and experience, and discussions with other trained law enforcement members of the INJTTF, I know that a person who uses a computer to access the internet and who chats and posts comments online, will often have content of their interests, such as, explosives and IED manufacturing, in their saved directories, book-marked websites, and electronic service provider data.

31. Based on my training and experience, and discussions with SABB McEuen, I know that, based on the detailed construction of the IED, the manufacturer(s) / designer(s) likely spent significant time on construction, experimentation and

Affidavit of John T. Slack

23 of 34

P10308DD.JHD.wpd

practice. Such manufacturer(s) / designer(s) commonly conduct experiments and practice runs to make sure the device functions properly. As a result, it is common that evidence of the use of an IED and/or propellant charges will result in post blast scenes. For this reason, the manufacturer(s) / designer(s) of an IED will commonly use rural areas to avoid detection by law enforcement or the general public. If the manufacturer(s) / designer(s) lives in a rural area, he/she may conduct such experiments and practice runs on their own property to avoid detection.

32. Based on my training and experience, and discussions with SABB McEuen, I know that the following items can be used to manufacture IEDs and may contain evidence of their possession, manufacture or use:

- a. Explosive materials, including high explosives such as dynamite, RDX based explosives, PETN, detonation cord, black powder, smokeless powder;
- b. Improvised explosives, including APAN, TATP, HMDT, EGDN and ANFO;
- c. Precursor chemicals to make explosives, including ammonium nitrate, hydrogen peroxide, acetone, acids, baking soda, Potassium chlorate, sodium chlorate, metal powders;
- d. Improvised explosive making tools, including filter, sieves, mixing bowls, items with chemical burns, work areas with burns and

Affidavit of John T. Slack

24 of 34

P10308DD.JHD.wpd



chemical burns, mixing bowls and utensils with explosive (energetic material) residue, scales, measuring spoons, pipes (metal and PVC);

- e. Timing, power units including, timing pieces, printed and non-printed circuit boards, soldering iron, solder, wire connectors, wires for conducting electricity, batteries, loads (nichrome wire, hobby rocket igniters, flash bulbs, broken bulbs, Christmas type bulbs (without Christmas decorations), hobby time fuse, military time fuse, improvised time fuse, sparklers, wireless transmitters and receivers, transistors, relays, ammunition primers, wire cutters, pliers, hammers, screw drivers, crimpers;
- f. Switch devices including, micro-switches, contact switches, motion detectors, passive infrared sensors, wire loops, pressure activated switches (positive and negative pressure);
- g. Shrapnel, including fishing weights, ball bearings, bb's; and
- h. Evidence of experimentation with IED's: torn/shredded materials, charred materials, explosively formed craters, shrapnel impacts on objects, expelled shrapnel (including fishing weights, ball bearings, bb's, and other similar metal objects), charred wire, and explosive residue.

33. Based on my training and experience, and discussions with SABT McEuen, I know that the following items can be used to research IEDs and may contain evidence of their possession, manufacture, use and may reveal the motivation or intent for their use:

- a. Any computer, computer system and related peripherals, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers,

Affidavit of John T. Slack

25 of 34

P10308DD.JHD.wpd

modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer-related operation equipment, digital cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to, hardware, software, diskettes, backup tapes, CD-ROM's, DVD's, flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict, describe the process of manufacturing IEDs, or instruct/encourage the use of, possession or threatened use an IED's;

- b. Books and magazines containing visual depictions, explosive recipes or the construction or use of concerning violations of the use, possession or threaten to use an IED;
- c. Originals, copies, and negatives of visual depictions of the use, possession or threaten to use an IED;
- d. Motion pictures, films, videos, and other recordings of visual depictions of the use, possession or threaten to use an IED;
- e. Information, electronic records, or correspondence pertaining to the possession, receipt, or use of explosives and/or IEDs and the motivation or intent for their use, including:
  - i. Registries regarding file-sharing software communications and participants in file-sharing Internet networks;
  - ii. Letters and other correspondence including, but not limited to

Affidavit of John T. Slack

26 of 34

P10308DD.JHD.wpd

electronic mail, chat logs, and electronic messages;

- iii. Books, ledgers, and records;
- iv. Chat logs, screen names, buddy lists; and
- v. Screen names and passwords for access to computers and encrypted sections thereof.

### DEFINITIONS

34. The following definitions apply to this Affidavit:

- a. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- b. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist

Affidavit of John T. Slack

27 of 34

P10308DD.JHD.wpd

of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- d. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image.
- g. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such

Affidavit of John T. Slack

28 of 34

P10308DD.JHD.wpd

as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

### BACKGROUND ON COMPUTERS AND THE INTERNET

35. Based on my knowledge and discussions with other trained law enforcement officers, computers, computer technology, and the Internet have revolutionized the manner in which information about explosives and the motivation and message that is being sent by their use is produced, distributed, and saved.

36. Based on my knowledge and discussions with other trained law enforcement officers by utilizing digital cameras images of use of explosives can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

37. A computer's ability to store images in digital form makes the computer itself an ideal repository for images of and information about the use, design, and manufacture of explosives. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images and documents at very high resolution.

38. The Internet affords individuals several different venues for meeting each other, obtaining, viewing and trading explosives information and ideologies in a relatively secure and anonymous fashion.

39. Individuals also use online resources to retrieve and store explosives information, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of explosives information is often found on the user's computer. Even in cases where online storage is used, however, evidence of explosive information can be found on the user's computer in most cases.

40. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving

Affidavit of John T. Slack

30 of 34

P10308DD.JHD.wpd

the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of

Affidavit of John T. Slack

31 of 34

P10308DD.JHD.wpd

storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

#### SPECIFICS OF SEARCH OF COMPUTER SYSTEMS

41. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to

Affidavit of John T. Slack

32 of 34

P10308DD.JHD.wpd



conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

42. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

### CONCLUSION

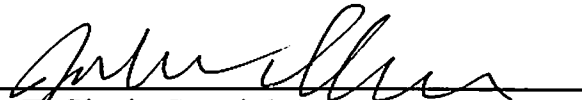
Based on the foregoing, your Affiant respectfully submits there is probable

Affidavit of John T. Slack


33 of 34

P10308DD.JHD.wpd

cause to conclude that Kevin William Harpham violated Title 18 U.S.C. § 2332a and Title 26 U.S.C. § 5861d. Accordingly, your Affiant respectfully requests that this Court find probable cause exists to support a criminal complaint charging Kevin William Harpham with the above-referenced crimes and to issue a warrant for his arrest.

  
\_\_\_\_\_  
John T. Slack, Special Agent  
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 8<sup>th</sup> day of March,  
2011.

  
\_\_\_\_\_  
Cynthia Imbrogno  
United States Magistrate Judge

Affidavit of John T. Slack

34 of 34

P10308DD.JHD.wpd